Operating System

Using the Delegation of Control Wizard

Beta 3 Technical Walkthrough

Abstract

This technical walkthrough shows specific examples of how to delegate control of objects in a Microsoft® Active Directory™ directory service folder, using the Delegation of Control Wizard in the Active Directory Users and Computers Manager.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0499

CONTENTS

INTRODUCTION

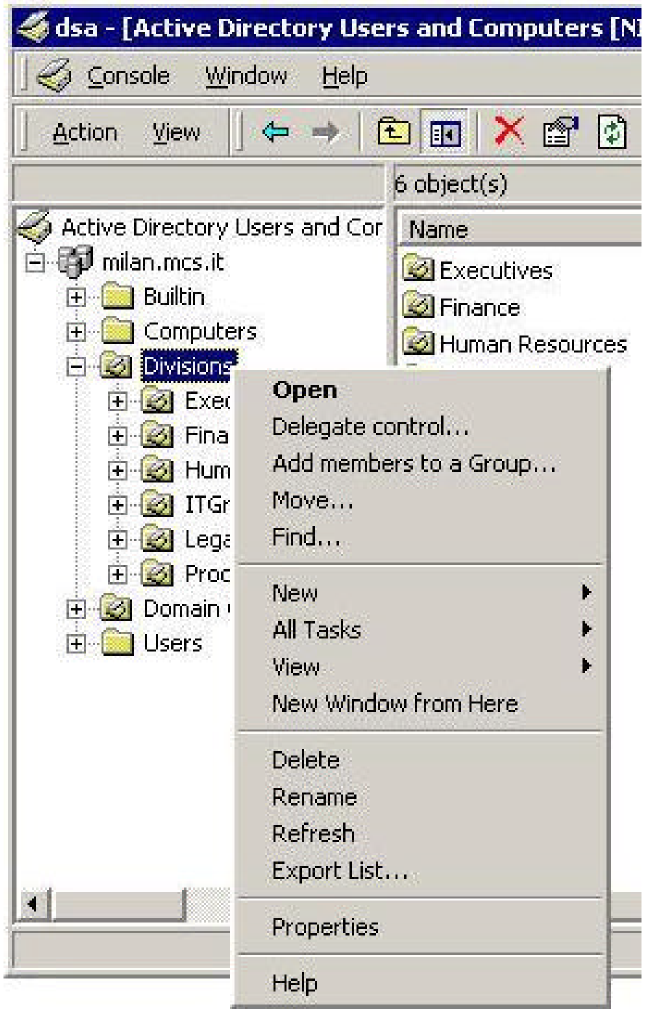
This technical walkthrough shows specific examples of how to delegate control of objects in a Microsoft® Active Directory™ folder using the Delegation of Control Wizard in the Active Directory Users and Computers Manager. Three examples illustrate the functionality:

- Delegate complete control of an organizational unit called *Autonomous Unit* to a group within the Autonomous Unit called *AUAdmins*.
- Delegate creation and deletion of users in an organizational unit called *Divisions* to a group called *HRTeam*.
- Delegate resetting of passwords for all users in an organizational unit called *Divisions* to a group called *HelpDesk*.

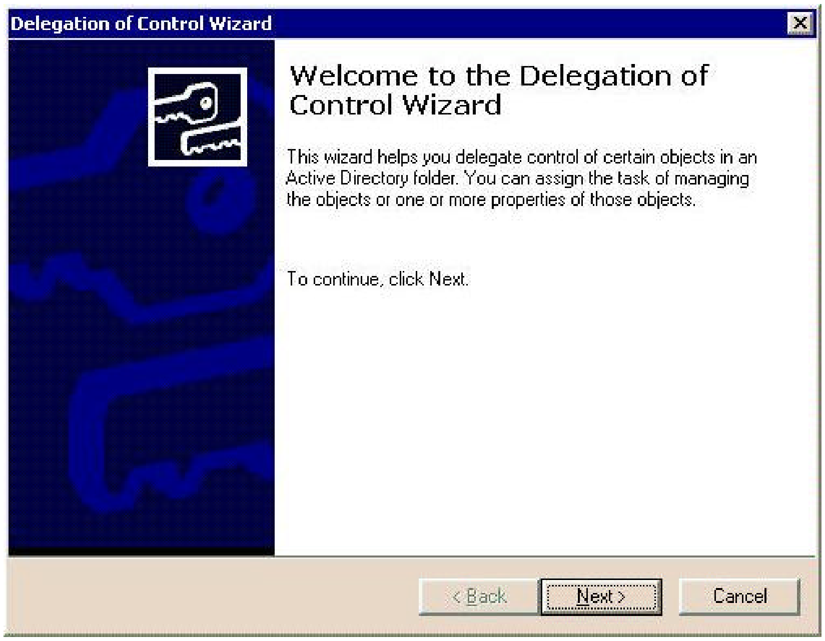
USING THE DELEGATION OF CONTROL WIZARD

To start the Delegation of Control Wizard

1. Select **Active Directory Users and Computers,** right-click on **Divisions**, and select **Delegate control….**



2. At the Welcome dialog box, click **Next** and follow the instructions.



Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of certain objects in an Active Directory folder. You can assign the task of managing the objects or one or more properties of those objects.

To continue, click Next.

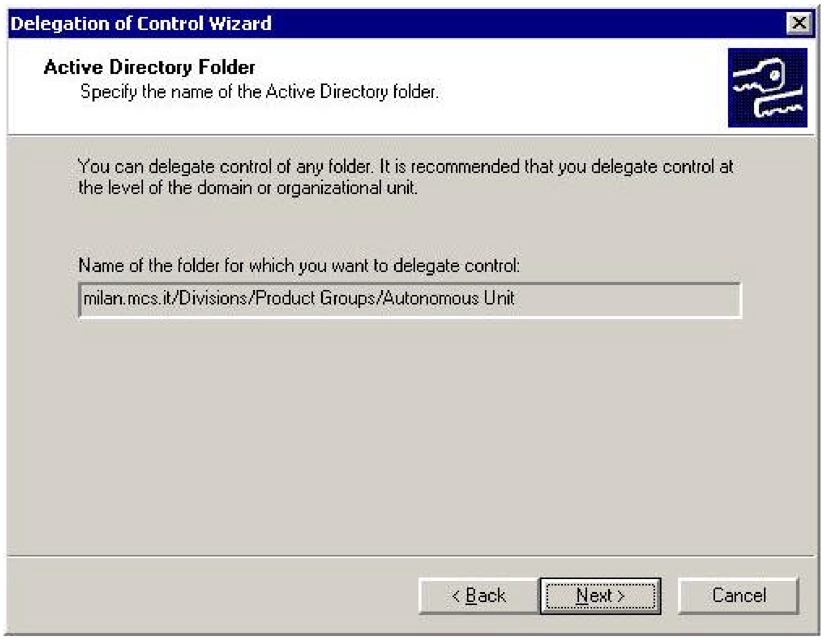
Delegate Complete Control of an Organizational Unit

This technical walkthrough represents a common task that large organizations may perform—delegate complete control of an organizational unit to some other group of administrators, thereby partitioning the control of the directory namespace.

To delegate control

1. Start **Active Directory Users and Computers**, and navigate to the organization unit (OU) on which you want to perform the delegation. In this case, it is the **Autonomous Unit** OU**.**

2. Right-click the OU name, and select **Delegate control.** The path of the delegated folder is shown below in the **Name of the folder for which you want to delegate control:** text entry box**.**



Delegation of Control Wizard

Active Directory Folder

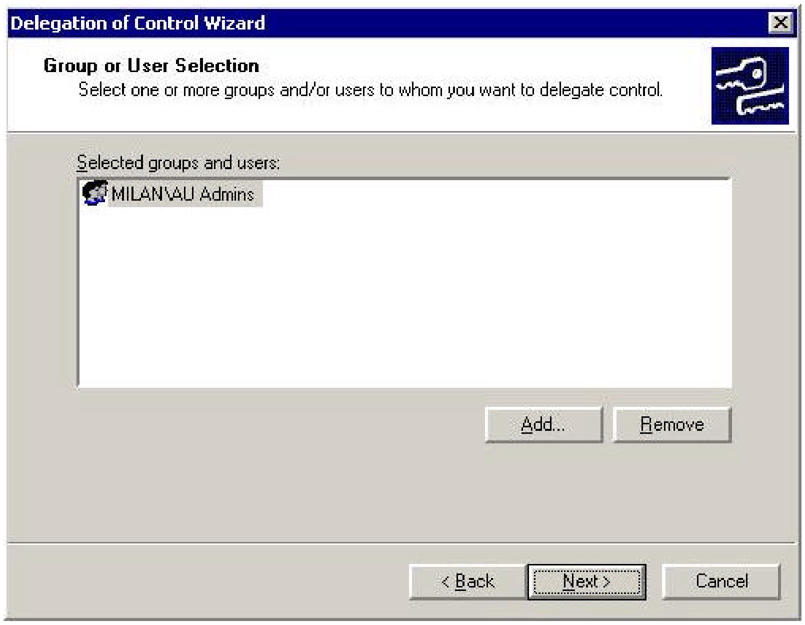
Specify the name of the Active Directory folder.

You can delegate control of any folder. It is recommended that you delegate control at the level of the domain or organizational unit.

Name of the folder for which you want to delegate control:

milan.mcs.it/Divisions/Product Groups/Autonomous Unit

3. On the **Group or User Selection** screen, select **AUAdmins** by clicking **Add.** Click **Next.**



Delegation of Control Wizard

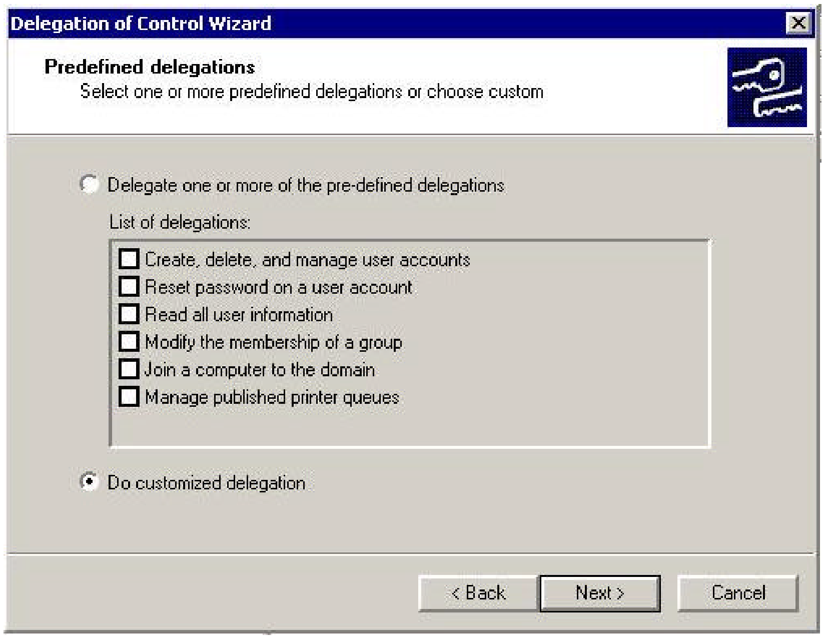
Group or User Selection

Select one or more groups and/or users to whom you want to delegate control.

Selected groups and users:

MILAN\AU Admins

4. Select **Do customized delegation**. This allows you to delegate control of the entire container. Click **Next.**



Delegation of Control Wizard

Predefined delegations

Select one or more predefined delegations or choose custom

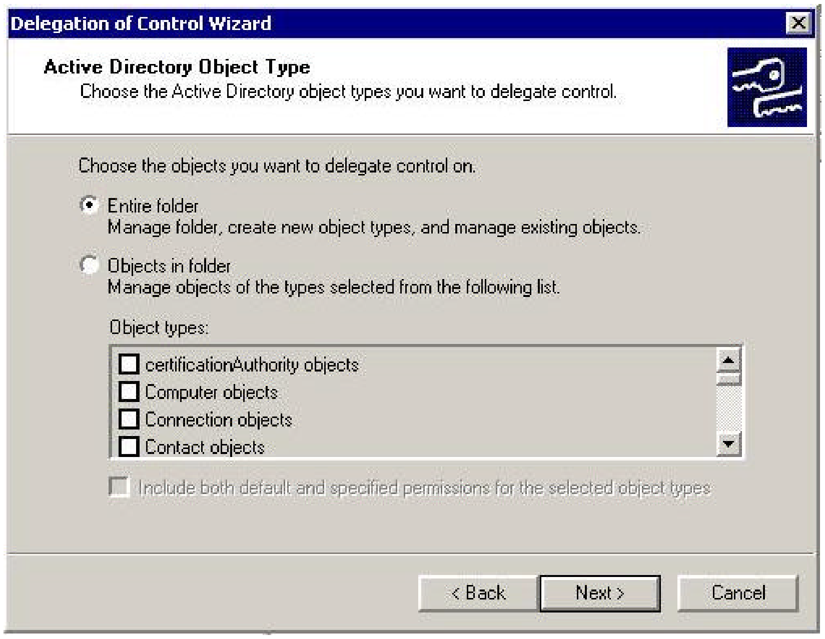
○ Delegate one or more of the pre-defined delegations

List of delegations:

□ Create, delete, and manage user accounts
□ Reset password on a user account
□ Read all user information
□ Modify the membership of a group
□ Join a computer to the domain
□ Manage published printer queues

● Do customized delegation

5. Select **Entire Folder.** Click **Next.**



Delegation of Control Wizard

Active Directory Object Type

Choose the Active Directory object types you want to delegate control.

Choose the objects you want to delegate control on.

● Entire folder
Manage folder, create new object types, and manage existing objects.

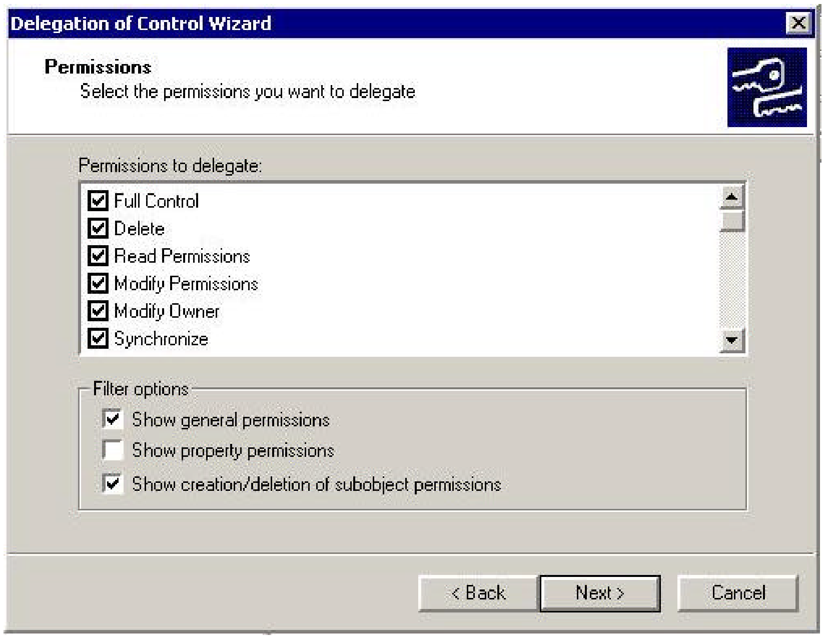
○ Objects in folder
Manage objects of the types selected from the following list.

Object types:

□ certificationAuthority objects
□ Computer objects
□ Connection objects
□ Contact objects

□ Include both default and specified permissions for the selected object types

6. Select **Full Control** to delegate complete control. Click **Next.**



Delegation of Control Wizard

Permissions

Select the permissions you want to delegate

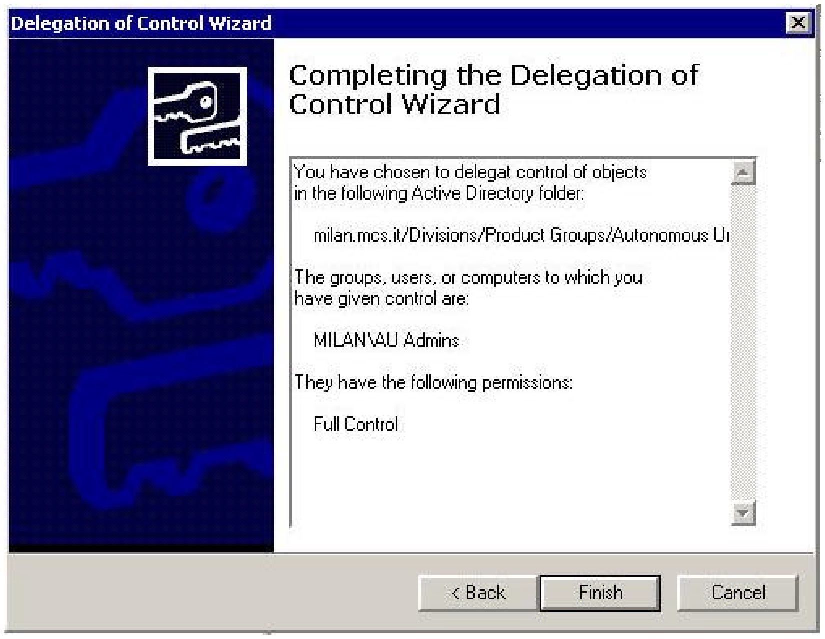
Permissions to delegate:

☑ Full Control
☑ Delete
☑ Read Permissions
☑ Modify Permissions
☑ Modify Owner
☑ Synchronize

Filter options

☑ Show general permissions
□ Show property permissions
☑ Show creation/deletion of subobject permissions

7. Click **Next** to see the summary dialog box. Click **Finish.**



Delegation of Control Wizard
Completing the Delegation of Control Wizard
< Back
Finish
Cancel

You have chosen to delegat control of objects in the following Active Directory folder:

milan.mcs.it/Divisions/Product Groups/Autonomous U

The groups, users, or computers to which you have given control are:

MILAN\AU Admins

They have the following permissions:

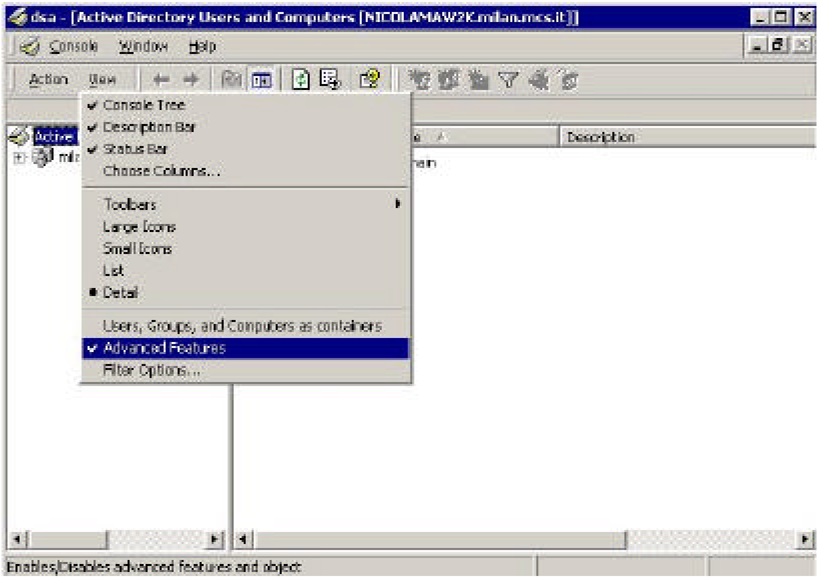
Full Control

Verify the Permissions Granted

Use the Access Control List (ACL) Editor to verify that you set permissions appropriately.

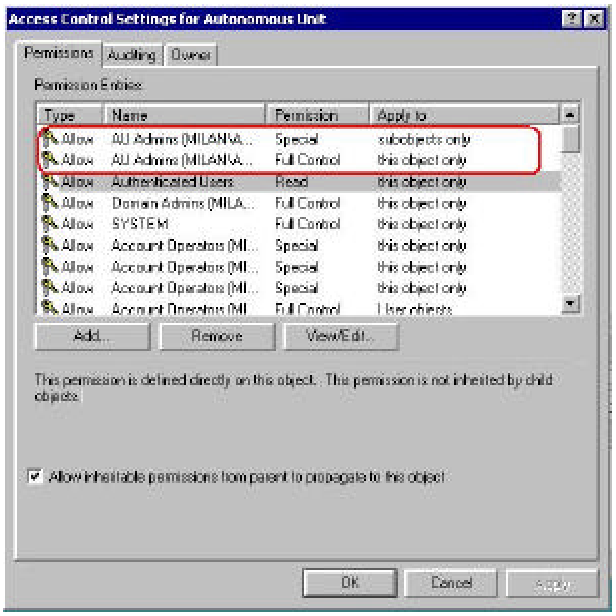
To verify permissions

1. Start the ACL Editor. Select **Active Directory Manager**. From the **View** menu, select **Advanced Features**.



Enables/Disables advanced features and object

2. Right-click the **Autonomous Unit** OU, and select **Properties**.
3. Select the **Security** tab and click **Advanced**. Select the **Permissions** tab, and note the several permission entries that apply to User objects. One of them is for **AUAdmins**.
4. Double-click **AUAdmins**, and you see that it gives full access on the OU and all its subobjects, that is the entire subtree. This indicates that permissions were granted correctly.



Permission Entries:

Type	Name	Permission	Apply to
Allow	AU Admins (MILANVA...	Special	subobjects only
Allow	AU Admins (MILANVA...	Full Control	this object only
Allow	Authenticated Users	Read	this object only
Allow	Domain Admins (MILA...	Full Control	this object only
Allow	SYSTEM	Full Control	this object only
Allow	Account Operators (MI...	Special	this object only
Allow	Account Operators (MI...	Special	this object only
Allow	Account Operators (MI...	Special	this object only
Allow	Account Operators (MI	Full Control	User objects

This permission is defined directly on this object. This permission is not inherited by child objects.

☑ Allow inheritable permissions from parent to propagate to this object

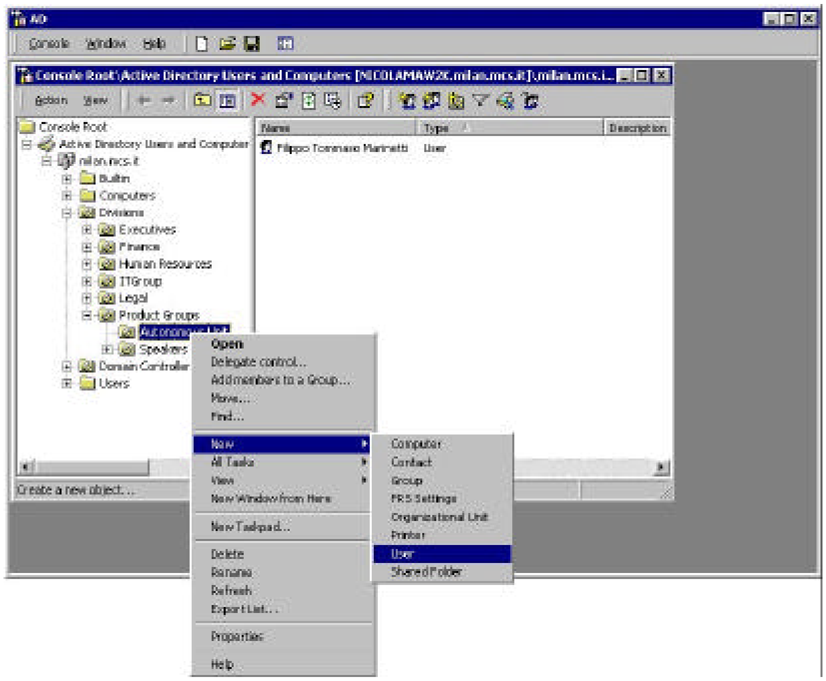
To verify the delegation

1. Log on to a user account that is a member of AUAdmins group.

   Note: You might not be able to log on interactively with this user if your machine is a Domain Controller. You must grant logon access to AUAdmins using the **Security Configuration and Analysis** Microsoft Management Console (MMC) snap-in.

2. Start **Active Directory Users and Computers.**

3. Attempt an arbitrary operation in the Autonomous Unit. For example, create a user using the **New** menu. The operation is successful. If you attempt a similar operation outside the OU, it fails and displays an Access Denied message. This confirms that the delegation was successful and is correctly scoped.

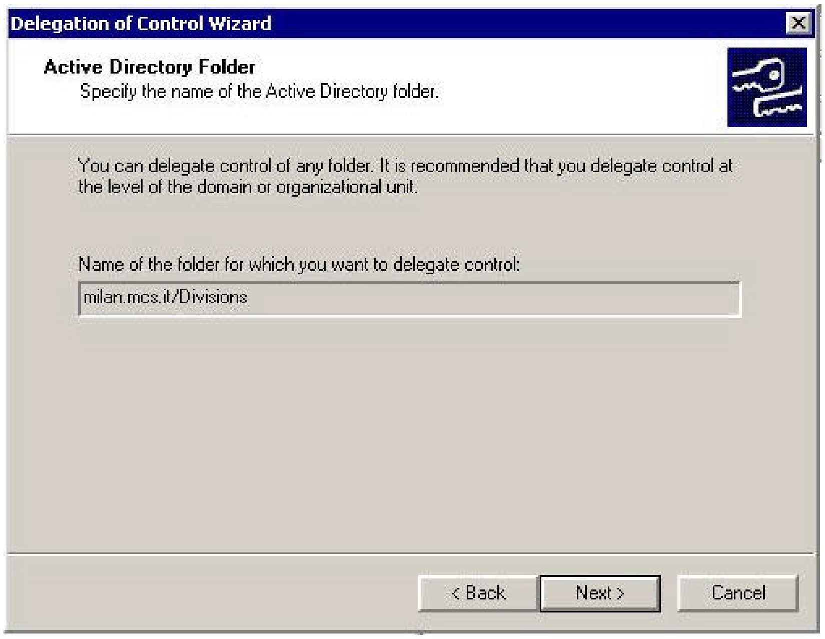

AD
Console Window Help
Console Root\Active Directory Users and Computers [NICOLAMAW2K.milan.mcs.it]\milan.mcs.i...
Action View
Console Root
Active Directory Users and Computer
milan.mcs.it
Builtin
Computers
Divisions
Executives
Finance
Human Resources
ITGroup
Legal
Product Groups
Autonomous Unit
Speakers
Domain Controller
Users
Name
Type
Description
Filippo Tommaso Marinetti
User
Open
Delegate control...
Add members to a Group...
Move...
Find...
New
All Tasks
View
New Window from Here
New Taskpad...
Delete
Rename
Refresh
Export List...
Properties
Help
Computer
Contact
Group
FRS Settings
Organizational Unit
Printer
User
Shared Folder
Create a new object...

Delegate Creation and Deletion of Users

This technical walkthrough represents another common task that large organizations perform—delegate the task of creating/deleting user accounts to the HRTeam, representing the Human Resources group. This delegation is at the next level of detail—giving object specific rights in the container, in this case the object is *User.*

To delegate creation and deletion of users

1. Start **Active Directory Users and Computers**, and select the organization unit you want to perform the delegation on. In this case it is the **Divisions** OU.
2. Right-click the OU name, and select **Delegate control…** The path of the delegated folder appears in the **Name of the folder for which you want to delegate control:** text box.



Delegation of Control Wizard

Active Directory Folder

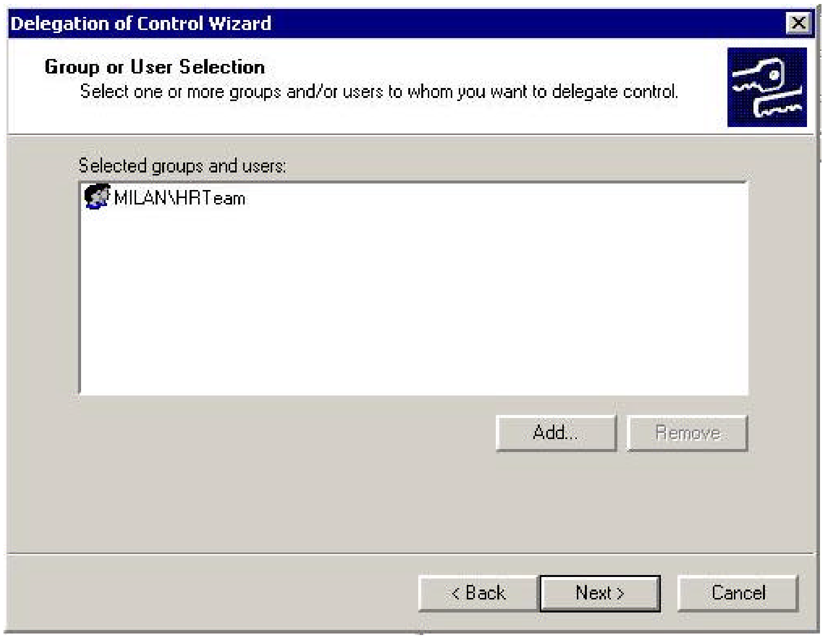
Specify the name of the Active Directory folder.

You can delegate control of any folder. It is recommended that you delegate control at the level of the domain or organizational unit.

Name of the folder for which you want to delegate control:

milan.mcs.it/Divisions

3. Select **HRTeam** and click **Add.**



Delegation of Control Wizard

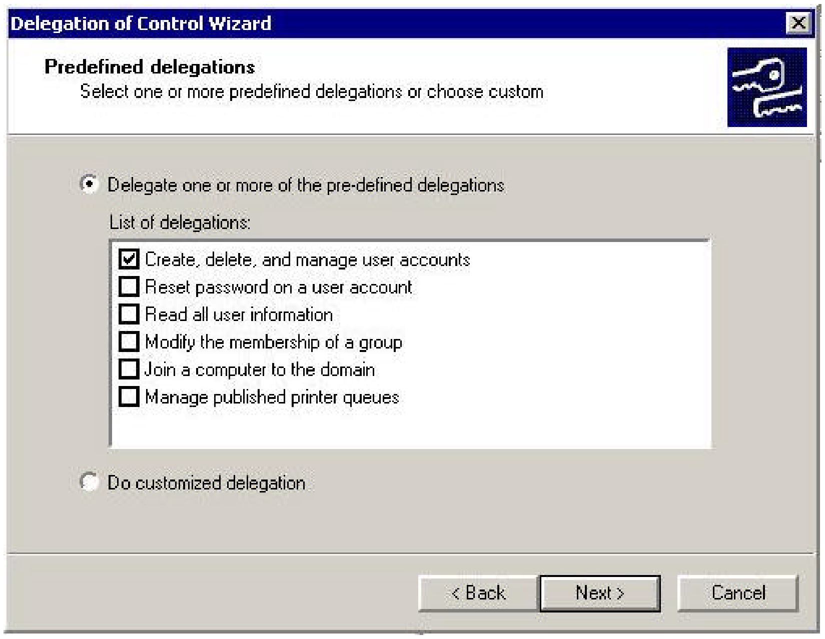
Group or User Selection

Select one or more groups and/or users to whom you want to delegate control.

Selected groups and users:

MILAN\HRTeam

4. Use one of the pre-defined delegations (the default). Select **Create, delete, and manage user accounts** to delegate creation/deletion of users in *this* container. Click **Next.**



Predefined delegations
Select one or more predefined delegations or choose custom

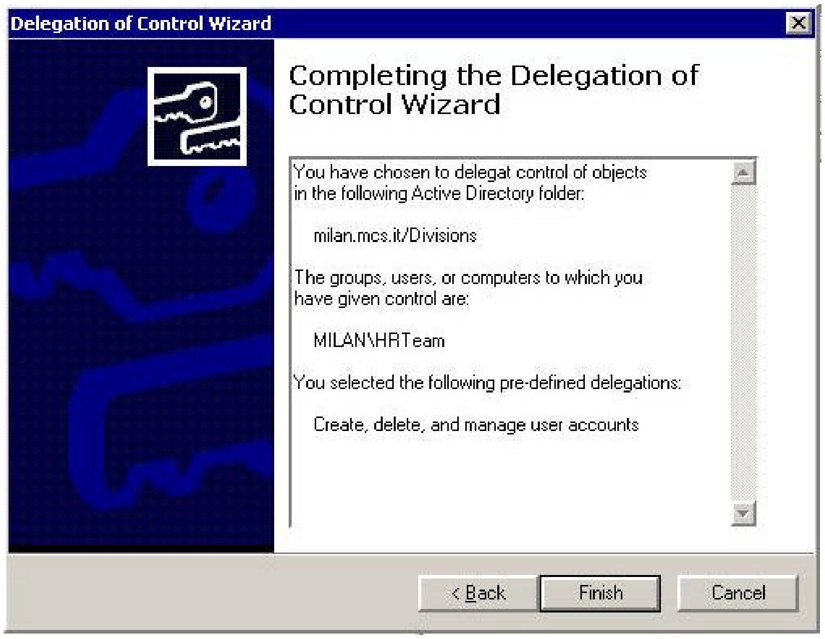
● Delegate one or more of the pre-defined delegations

List of delegations:

☑ Create, delete, and manage user accounts
□ Reset password on a user account
□ Read all user information
□ Modify the membership of a group
□ Join a computer to the domain
□ Manage published printer queues

○ Do customized delegation

5. Click **Next** to see the summary dialog box. Click **Finish.**



Completing the Delegation of Control Wizard

You have chosen to delegat control of objects
in the following Active Directory folder:

milan.mcs.it/Divisions

The groups, users, or computers to which you
have given control are:

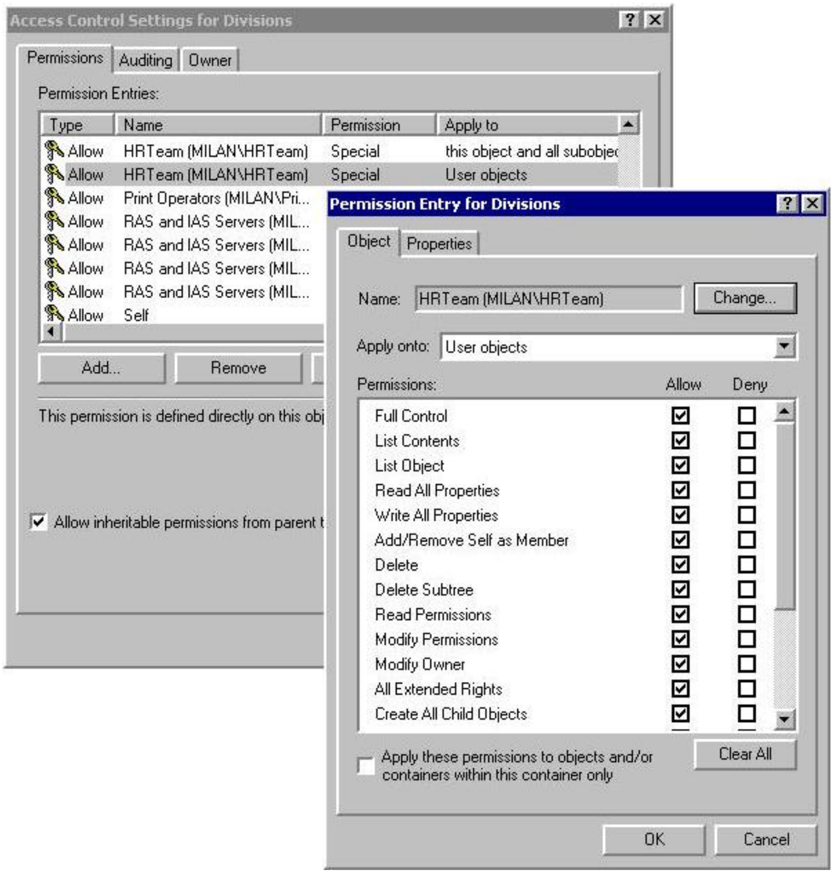
MILAN\HRTeam

You selected the following pre-defined delegations:

Create, delete, and manage user accounts

To verify the permissions granted

1. Start the ACL Editor. Select **Active Directory Users and Computers**. From the **View** menu, select **Advanced Features.**
2. Right-click the **Divisions** OU, and select **Properties**.
3. Select the **Security** tab, and click **Advanced**. You see several permission entries that apply to user objects, including one for **HRTeam**.
4. Double-click **HRTeam**, and you see that it gives **Create User objects** and **Delete User objects** rights to HRTeam in the container (Divisions OU) and all sub-objects (entire subtree under the OU). This indicates that task was completed successfully.



Permission Entries:

Type	Name	Permission	Apply to
Allow	HRTeam (MILAN\HRTeam)	Special	this object and all subobjec
Allow	HRTeam (MILAN\HRTeam)	Special	User objects
Allow	Print Operators (MILAN\Pri...		
Allow	RAS and IAS Servers (MIL...		
Allow	RAS and IAS Servers (MIL...		
Allow	RAS and IAS Servers (MIL...		
Allow	RAS and IAS Servers (MIL...		
Allow	Self		

This permission is defined directly on this obj

☑ Allow inheritable permissions from parent t

Name: HRTeam (MILAN\HRTeam)

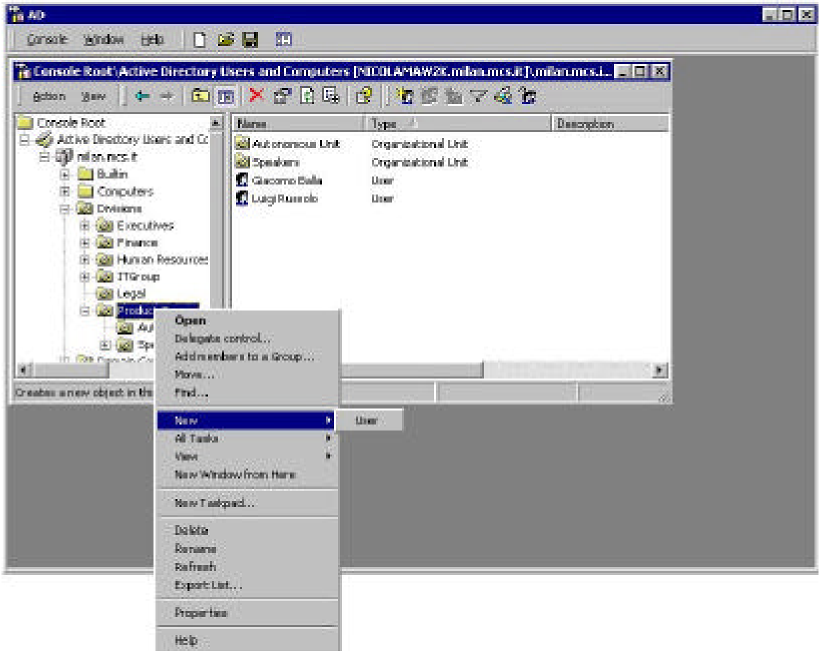
Apply onto: User objects

Permissions:	Allow	Deny
Full Control	☑	□
List Contents	☑	□
List Object	☑	□
Read All Properties	☑	□
Write All Properties	☑	□
Add/Remove Self as Member	☑	□
Delete	☑	□
Delete Subtree	☑	□
Read Permissions	☑	□
Modify Permissions	☑	□
Modify Owner	☑	□
All Extended Rights	☑	□
Create All Child Objects	☑	□

□ Apply these permissions to objects and/or containers within this container only

To verify the delegation

1. Log on to a user account that is member of HelpDesk group.
2. Start **Active Directory Users and Computers**, and select any OU within the **Divisions** OU.
3. Right-click and select **New.** On the submenu, you see **User,** the option to create a new user.
4. This verifies that you can create users as member of HelpDesk group now.



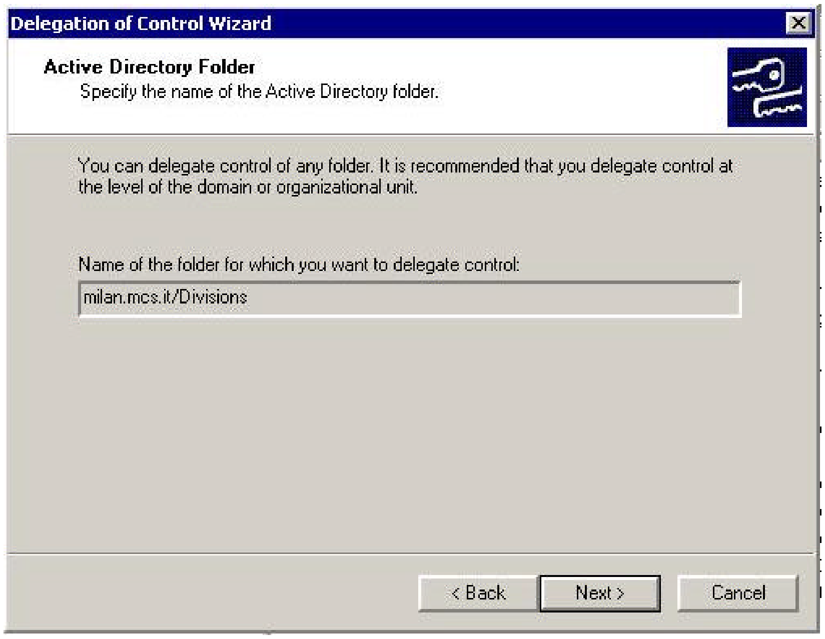
Name	Type	Description
Autonomous Unit	Organizational Unit	
Speakers	Organizational Unit	
Giacomo Balla	User	
Luigi Russolo	User	

Delegate Resetting of Passwords for All Users

This technical walkthrough represents an important task that large organizations perform—delegate the task of resetting passwords on user accounts when users forget them and call into the HelpDesk team.

To delegate resetting of passwords

1. Start **Active Directory Users and Computers**, and select the organization unit you want to perform the delegation on. In this case, it is the **Divisions** OU.
2. Right-click **Divisions**, and select **Delegate control…**. The path of the delegated folder appears in **Name of the folder for which you want to delegate control:** text box.



Delegation of Control Wizard

Active Directory Folder

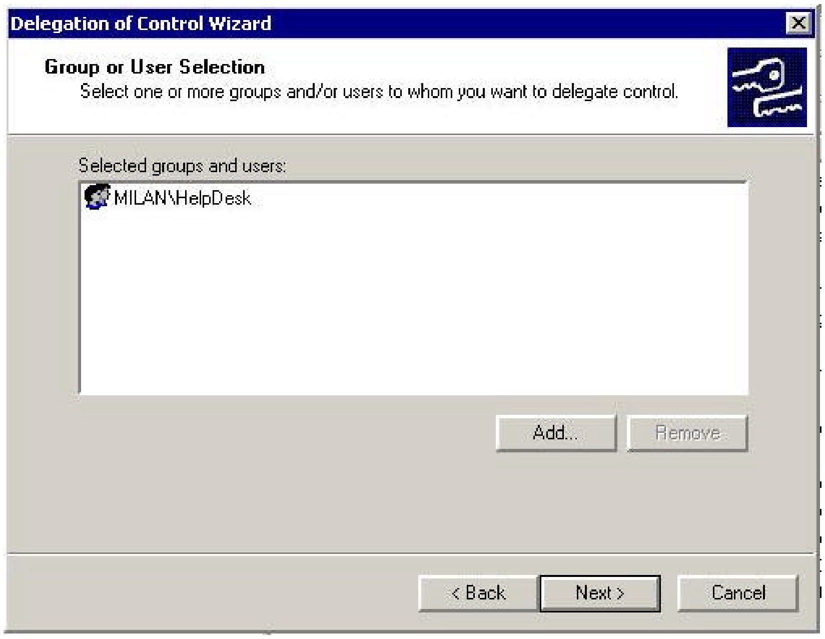
Specify the name of the Active Directory folder.

You can delegate control of any folder. It is recommended that you delegate control at the level of the domain or organizational unit.

Name of the folder for which you want to delegate control:

milan.mcs.it/Divisions

3. Select **HelpDesk** by clicking **Add**.



Delegation of Control Wizard

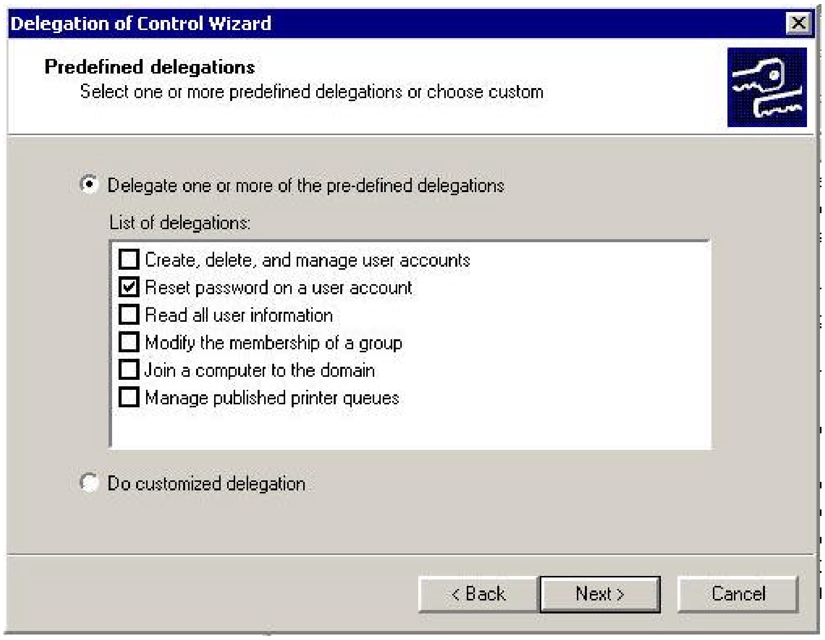
Group or User Selection

Select one or more groups and/or users to whom you want to delegate control.

Selected groups and users:

MILAN\HelpDesk

4. Again, you should use one of the pre-defined delegations (the default). Select **Reset password on a user accounts**, as shown in the picture below. Click **Next**.



Delegation of Control Wizard

Predefined delegations

Select one or more predefined delegations or choose custom

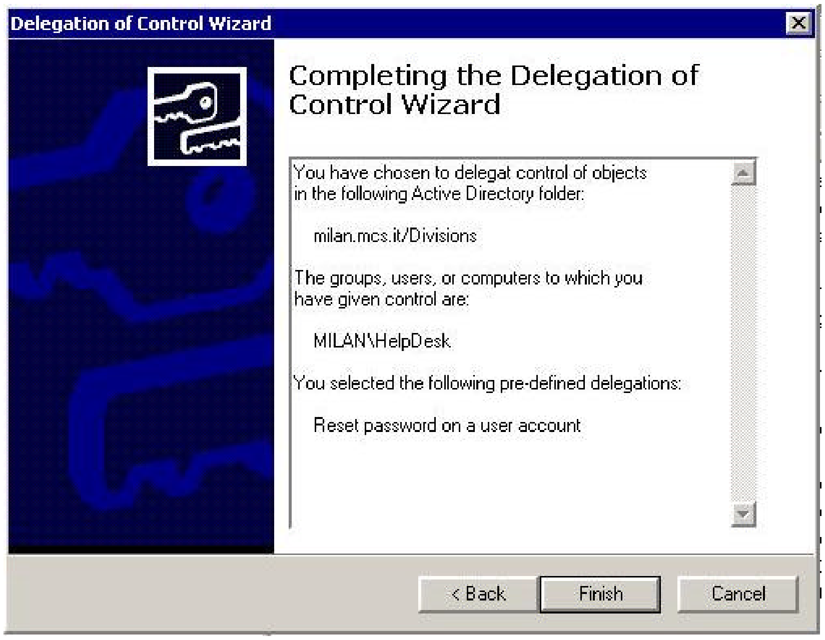
● Delegate one or more of the pre-defined delegations

List of delegations:

- □ Create, delete, and manage user accounts
- ☑ Reset password on a user account
- □ Read all user information
- □ Modify the membership of a group
- □ Join a computer to the domain
- □ Manage published printer queues

○ Do customized delegation

5. Click **Finish.**



Completing the Delegation of Control Wizard

You have chosen to delegat control of objects in the following Active Directory folder:

milan.mcs.it/Divisions

The groups, users, or computers to which you have given control are:

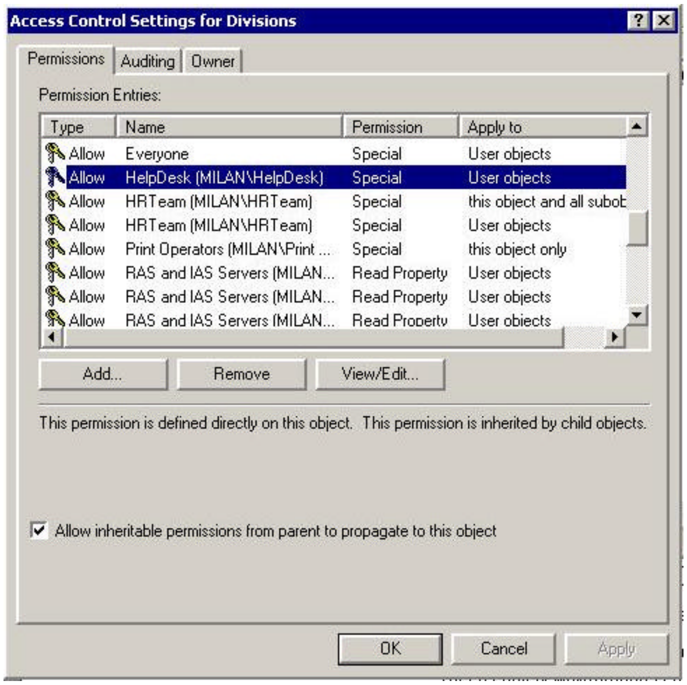
MILAN\HelpDesk

You selected the following pre-defined delegations:

Reset password on a user account

To verify the permissions granted

1. Start the ACL Editor. Select **Active Directory Users and Computers.** From the **View** menu, and select **Advanced Features**.
2. Right-click the **Divisions** OU, and select **Properties**.
3. Select the **Security** tab, and click **Advanced**. You should see several permission entries that apply to User objects. One of them is for **HelpDesk**.



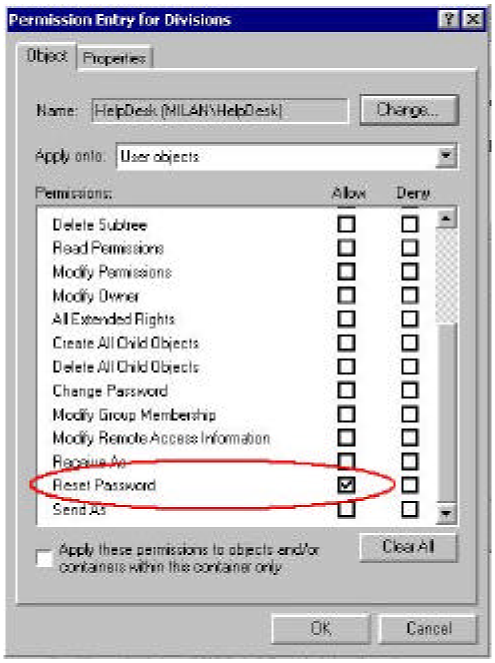
Permission Entries:

Type	Name	Permission	Apply to
Allow	Everyone	Special	User objects
Allow	HelpDesk (MILAN\HelpDesk)	Special	User objects
Allow	HRTeam (MILAN\HRTeam)	Special	this object and all subot
Allow	HRTeam (MILAN\HRTeam)	Special	User objects
Allow	Print Operators (MILAN\Print ...	Special	this object only
Allow	RAS and IAS Servers (MILAN...	Read Property	User objects
Allow	RAS and IAS Servers (MILAN...	Read Property	User objects
Allow	RAS and IAS Servers (MILAN...	Read Property	User objects

This permission is defined directly on this object. This permission is inherited by child objects.

☑ Allow inheritable permissions from parent to propagate to this object

4. Double-click **HelpDesk** and you should see that it gives *Reset Password* right on user objects. This indicates that task was performed. All the other permissions that apply to user objects are the defaults that were picked from the schema.



Name: HelpDesk (MILAN\HelpDesk)

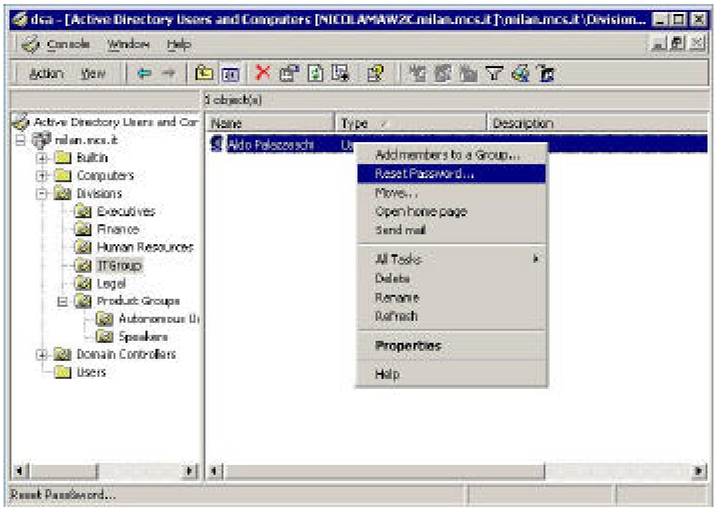
Apply onto: User objects

Permissions:	Allow	Deny
Delete Subtree	□	□
Read Permissions	□	□
Modify Permissions	□	□
Modify Owner	□	□
All Extended Rights	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Change Password	□	□
Modify Group Membership	□	□
Modify Remote Access Information	□	□
Receive As	□	□
Reset Password	☑	□
Send As	□	□

□ Apply these permissions to objects and/or containers within this container only

To verify the delegation

1. Log on to a user account that is member of HelpDesk group.
2. Start **Active Directory Users and Computers**, and select any user within **Divisions** OU.
3. Right-click the user name, and select **Reset Password**. The password is reset.
4. Try the same operation on a user outside Divisions OU. The reset attempt fails, and an *Access Denied* message is displayed. This confirms that the delegation was successful and is correctly scoped.



Variations to the Delegation Task

This technical walkthrough is an example of the highest level of control that can be delegated in Active Directory—one operation that applies to objects of certain type is delegated within a specific OU. There are several other variations that may be interesting:

- Instead of delegating a control right such *as* **Reset Password***,* you may want to delegate ability to read/write telephone number attributes for all **User** objects to a group called Receptionist. If you try this walkthrough, the differences are:
  - You have to use a customized delegation; the pre-defined ones do not suffice.
  - You must select the **User** object and choose **Phone and Mail Options**.
  - Additionally, to see property specific rights, you must select the **Show General Permissions** check box and clear the **Show Property Permissions** and **Show creation/deletion of subobjects permissions** check boxes. These check boxes allow you to see different types of rights that you can grant. Because the list of rights can be extremely large, these check boxes allow you to filter interesting rights.
- Instead of delegating a control right such as **Reset Password***,* you may want to delegate full access on all user objects to a group called **NetAccounts***.* If you try this walkthrough, you must choose **Full Control** instead of **Reset Password***.*

  Note: This is a distinction from the delegation done to HRTeam for creation/deletion of user objects in the second example above. In this instance, you have delegated management of existing accounts to NetAccounts but they still can t create new accounts. HRTeam can create new accounts but do not manage them.
- Another variation could be to delegate ability to manage printers under Computer objects in the Print Servers OU to printer admins, using the pre-defined delegation.

FOR MORE INFORMATION

For the latest information on Microsoft Windows 2000 network operating system, visit our World Wide Web site at http://www.microsoft.com/windows/server/ and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows 2000 Beta 3, visit the World Wide Web site at http://ntbeta.microsoft.com/.

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported via the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce it and fix it. Refer to the Release Notes included on the Windows 2000 Beta 3 distribution media for some of the known issues.